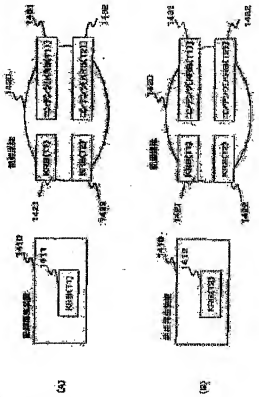
INFORMATION RECORDING DEVICE, INFORMATION REPRODUCING DEVICE, INFORMATION RECORDING METHOD, INFORMATION REPRODUCING METHOD, AND INFORMATION RECORDING MEDIUM, AND PROGRAM PROVIDING MEDIUM

Publication number: JP2002009753 (A)
Publication date: 2002-01-11
Inventor(s): ASANO TOMOYUKI; OSAWA YOSHITOMO; ISHIGURO RYUJI; MITSUZAWA ATSUSHI; OISHI TAKEO +
Applicant(s): SONY CORP +
Classification:
- International: ***G06F12/14; G06F21/24; G09C1/00; G11B20/10; H04L9/08;*** **G06F12/14; G06F21/00; G09C1/00; G11B20/10; H04L9/08;** (IPC1-7): G06F12/14; G09C1/00; G11B20/10; H04L9/08
- European:
Application number: JP20000186174 20000621
Priority number(s): JP20000186174 20000621

Also published as:
JP3988358 (B2)

Abstract of **JP 2002009753 (A)**

PROBLEM TO BE SOLVED: To provide an information recording and reproducing device and its method that selectively use a key revision block (KRB) of the newest version so as to encrypt contents and store them to a recording medium. SOLUTION: The method is configured to store KRBs having different generations and versions to a recording medium. In the case of detecting the newest KRB, it is stored in a memory in the recording and reproducing device. In the contents storage processing to the recording medium, newest available KRBs are detected among KRBs in the memory of the recording and reproducing device and KRBs on the recording medium to acquire an encryption processing key such as a media key and to execute encryption processing for the contents. Thus, it is possible to store encrypted contents on the basis of a KRB of a newer version to the recording medium at all times.



Data supplied from the ***espacenet*** database — Worldwide

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－9753
（Ｐ2002－9753Ａ）
(43)公開日　平成14年１月11日(2002.1.11)

(51)Int.Cl.'	識別記号	Ｆ Ｉ		テーマコード'(参考)
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０９Ｃ　1/00	６６０Ｄ	５Ｄ０４４
Ｇ０９Ｃ　1/00	６６０	Ｇ１１Ｂ　20/10	Ｈ	５Ｊ１０４
Ｇ１１Ｂ　20/10		Ｈ０４Ｌ　9/00	６０１Ｂ	

審査請求　未請求　請求項の数20　ＯＬ　（全 31 頁）

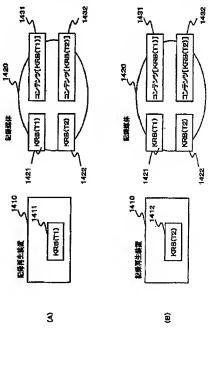
(21)出願番号　特願2000－186174(Ｐ2000－186174)
(22)出願日　平成12年６月21日(2000.6.21)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　大澤　毅知
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体

(57)【要約】
【課題】　最新バージョンのキー更新ブロック（ＫＲＢ）を選択的に使用してコンテンツを暗号化して記録媒体に格納する情報記録再生装置および方法を提供する。
【解決手段】　複数の異なる世代、バージョンを持つＫＲＢを記録媒体に格納する構成とした。さらに、最新のＫＲＢを検出した場合は、記録再生装置内のメモリに格納する。記録媒体へのコンテンツ格納処理においては、記録再生装置のメモリ内のＫＲＢ、記録媒体上の複数のＫＲＢ中から、利用可能な最新ＫＲＢを検出して暗号処理用キー、例えばメディアキーを取得して、コンテンツの暗号処理を実行する。従って、常により新しいバージョンのＫＲＢに基づく暗号化コンテンツを記録媒体に格納することが可能となる。



3　(6)

1

【特許請求の範囲】

【請求項１】記録媒体に情報を記録する情報記録装置において、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーを格納し、前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成される第一更新ブロック（ＫＲＢ）を格納するメモリ手段と、

前記情報記録装置に内蔵した前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能な第一更新ブロック（ＫＲＢ）の復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に対する格納データの暗号化処理を実行する暗号処理手段と、を有し、

前記暗号処理手段は、

前記記録媒体に対するコンテンツの暗号化および格納処理において、記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報記録装置自身のメモリに格納した第一更新ブロック（ＫＲＢ）中から利用可能な最新のキー更新ブロック（ＫＲＢ）を検出して、検出した利用可能な最新のキー更新ブロック（ＫＲＢ）の復号処理によって得られる暗号処理用キーを用いて記録媒体に対する格納データの暗号化処理を実行する構成を有することを特徴とする情報記録装置。

【請求項２】前記暗号処理用キーは、複数の情報記録装置に共通なマスターキー、情報記録装置に固有のデバイスキー、記録媒体に固有に設定されるメディアキーのいずれかであることを特徴とする請求項１に記載の情報記録装置。

【請求項３】前記情報記録装置は、さらに、

記録媒体に格納された第一更新ブロック（ＫＲＢ）、および情報記録装置自身の有するキー更新ブロック（ＫＲＢ）中の利用可能な最新のキー更新ブロック（ＫＲＢ）が、情報記録装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）であり、該最新のキー更新ブロック（ＫＲＢ）が記録媒体に未格納である場合において、記録媒体に対する前記最新のキー更新ブロック（ＫＲＢ）の書き込み処理を実行する構成を有することを特徴とする請求項１に記載の情報記録装置。

【請求項４】前記情報記録装置は、さらに、

記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報記録装置自身の有するキー更新ブロック（ＫＲＢ）中の利用可能な最新のキー更新ブロック（ＫＲＢ）が、記録媒体に格納したキー更新ブロック（ＫＲＢ）であり、該最新のキー更新ブロック（ＫＲＢ）が情報記録装置自身のメモリに未格納である場合において、情報記録装置自身のメモリに対する前記最新のキー更新ブロック（ＫＲＢ）の書き込み処理を実行する構成を有することを特徴とする請求項１に記載の情報記録装置。

2

【請求項５】前記ノードキーは更新可能なキーとして構成され、前記暗号処理用キー更新処理に際して、更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した第一更新ブロック（ＫＲＢ）を暗号処理用キー提供対象リーフの情報記録装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した暗号処理用キーを受領し、

キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、既取得した更新ノードキーに基づいて前記暗号処理用キーを算出する構成を有することを特徴とする請求項１に記載の情報記録装置。

【請求項６】前記暗号処理用キーは、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする請求項１に記載の情報記録装置。

【請求項７】記録媒体から情報を再生する情報再生装置において、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーを格納し、前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成される第一更新ブロック（ＫＲＢ）を格納するメモリ手段と、

前記情報再生装置に内蔵した前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能な第一更新ブロック（ＫＲＢ）の復号処理を実行して、前記記録媒体に格納された暗号データの復号処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に格納された暗号データの復号処理を実行する暗号処理手段と、を有し、

前記暗号処理手段は、

前記記録媒体に格納された暗号データの復号処理において、記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報再生装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック（ＫＲＢ）を検出して、検出したキー更新ブロック（ＫＲＢ）の復号処理によって得られる暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行する構成を有することを特徴とする情報再生装置。

【請求項８】前記暗号処理用キーは、複数の情報再生装置に共通なマスターキー、情報再生装置に固有のデバイスキー、記録媒体に固有に設定されるメディアキーのいずれかであることを特徴とする請求項７に記載の情報再生装置。

【請求項９】前記情報再生装置は、さらに、

記録媒体に格納されたキー更新ブロック（ＫＲＢ）、お

および情報再生装置自身の有するキー更新ブロック（ＫＲＢ）中の利用可能な最新のキー更新ブロック（ＫＲＢ）が、記録媒体に格納したキー更新ブロック（ＫＲＢ）であり、該最新のキー更新ブロック（ＫＲＢ）が情報再生装置自身のメモリに未格納である場合において、情報再生装置自身のメモリに対する前記最新のキー更新ブロック（ＫＲＢ）の書き込み処理を実行する構成を有することを特徴とする請求項７に記載の情報再生装置。

【請求項１０】前記ノードキーは更新可能なキーとして構成され、前記暗号処理用キー更新処理に際して、更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を暗号処理用キー提供対象リーフの情報再生装置に配布する構成であり、

前記情報再生装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した暗号処理用キーを受領し、

キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号処理用キーを算出する構成を有することを特徴とする請求項７に記載の情報再生装置。

【請求項１１】前記暗号処理用キーは、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする請求項７に記載の情報再生装置。

【請求項１２】複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録装置における情報記録方法であり、

記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報記録装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）中から利用可能な最新のキー更新ブロック（ＫＲＢ）を検出するＫＲＢ検出ステップと、

前記ＫＲＢ検出ステップにおいて、検出された利用可能な最新のキー更新ブロック（ＫＲＢ）について、前記情報記録装置に内蔵したノードキーまたはリーフキーの少なくともいずれかを用いてキー更新ブロック（ＫＲＢ）の復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行するＫＲＢ復号処理ステップと、

前記ＫＲＢ復号処理ステップにおいて、算出された暗号処理用キーを用いて前記記録媒体に対する記録データの暗号化を行ない記録媒体に格納するステップと、

を有することを特徴とする情報記録方法。

【請求項１３】前記情報記録方法において、

前記ＫＲＢ検出ステップにおいて、検出した利用可能な最新のキー更新ブロック（ＫＲＢ）が、情報記録装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）であり、該最新のキー更新ブロック（ＫＲＢ）が記録媒体に未格納である場合において、記録媒体に対する前記最新のキー更新ブロック（ＫＲＢ）の書き込み処理を実行することを特徴とする請求項１２に記載の情報記録方法。

【請求項１４】前記情報記録方法において、

前記ＫＲＢ検出ステップにおいて、検出した利用可能な最新のキー更新ブロック（ＫＲＢ）が、記録媒体に格納したキー更新ブロック（ＫＲＢ）であり、該最新のキー更新ブロック（ＫＲＢ）が情報記録装置自身のメモリに未格納である場合において、情報記録装置自身のメモリに対する前記最新のキー更新ブロック（ＫＲＢ）の書き込み処理を実行することを特徴とする請求項１２に記載の情報記録方法。

【請求項１５】複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を行なう情報再生装置における情報再生方法であり、

記録媒体に格納され、再生対象となるコンテンツの暗号処理用キーのバージョン情報を取得するステップと、

記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報再生装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック（ＫＲＢ）を検出する検出ステップと、

前記検出ステップにおいて検出したキー更新ブロック（ＫＲＢ）の復号処理によって暗号処理用キーを生成するステップと、

生成した暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行するステップと、

をなすことを特徴とする情報再生方法。

【請求項１６】前記情報再生方法において、

前記ＫＲＢ検出ステップにおいて、検出した利用可能な最新のキー更新ブロック（ＫＲＢ）が、記録媒体に格納したキー更新ブロック（ＫＲＢ）であり、該最新のキー更新ブロック（ＫＲＢ）が情報再生装置自身のメモリに未格納である場合において、情報再生装置自身のメモリに対する前記最新のキー更新ブロック（ＫＲＢ）の書き込み処理を実行することを特徴とする請求項１５に記載の情報再生方法。

【請求項１７】情報を記録可能な情報記録媒体であって、

複数の異なる情報記録装置または情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置または再生装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を、異なる構成を持つ複数のキー更新ブロック（ＫＲＢ）として、格納したことを特徴とする情報記録媒体。

【請求項１８】前記複数のキー更新ブロック（ＫＲＢ）

の各々は、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする請求項１７に記載の情報記録媒体。

【請求項１９】複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録装置における情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報記録装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）中から利用可能な最新のキー更新ブロック（ＫＲＢ）を検出するＫＲＢ検出ステップと、

前記ＫＲＢ検出ステップにおいて、検出された利用可能な最新のキー更新ブロック（ＫＲＢ）について、前記情報記録装置に内蔵したノードキーまたはリーフキーの少なくともいずれかを用いてキー更新ブロック（ＫＲＢ）の復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行するＫＲＢ復号処理ステップと、

前記ＫＲＢ復号処理ステップにおいて、算出された暗号処理用キーを用いて前記記録媒体に対する記録データの暗号化を行ない記録媒体に格納するステップと、

をなすことを特徴とするプログラム提供媒体。

【請求項２０】複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を行なう情報再生装置における情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

記録媒体に格納され、再生対象となるコンテンツの暗号処理用キーのバージョン情報を取得するステップと、

記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報再生装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック（ＫＲＢ）を検出する検出ステップと、

前記検出ステップにおいて検出したキー更新ブロック（ＫＲＢ）の復号処理によって暗号処理用キーを生成するステップと、

生成した暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行するステップと、

をなすことを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関し、木構造の階層の鍵配信方式を用いてマスターキーあるいはメディアキー等の暗号鍵更新を行ない、さらに、記録媒体に新たに格納されるコンテンツに関して、より新しいキーを用いた暗号化を可能とした構成に関する。具体的には、各記録再生器機器をｎ分の各葉（リーフ）に配置した構成の鍵配信方法を用い、コンテンツの配信、再生に必要な鍵を配信するとともに、複数の世代、バージョンの異なるキーを記録媒体に格納し、新たに格納するコンテンツに対する暗号化処理の際に、より新しいキーを検出して、これを用いて配録を行う構成とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関する。

【０００２】

【従来の技術】ディジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、ディジタル的に記録する記録装置や記録媒体が普及しつつある。このようなディジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにディジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなディジタルデータの不正なコピーを防ぐため、ディジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

【０００３】例えば、ＭＤ（ミニディスク）（ＭＤは商標）装置において、違法なコピーを防止する方法として、ＳＣＭＳ(Serial Copy Management System)が採用されている。ＳＣＭＳは、データ再生側において、オーディオデータとともにＳＣＭＳ信号をディジタルインタフェース（ＤＩＦ）から出力し、データ記録側において、再生側からのＳＣＭＳ信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【０００４】具体的にはＳＣＭＳ信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、１度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、ＤＩＦからオーディオデータを受信すると、そのオーディオデータとともに送信されるＳＣＭＳ信号を検出する。そして、ＳＣＭＳ信号が、コピーフリー（copy free）となっている場合には、オーディオデータをＳＣＭＳ信号とともにミニディスクに記録する。また、ＳＣＭＳ信号が、コピーを１度のみ許可（copy once allowed）となっている場合には、ＳＣＭＳ信号をコピー禁止（copy p

rohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、ＳＣＭＳ信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなＳＣＭＳを使用した制御を行なうことで、ミニディスク装置では、ＳＣＭＳによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【０００５】しかしながら、ＳＣＭＳは上述のようにＳＣＭＳ信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、ＳＣＭＳの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、ＤＶＤプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

【０００６】コンテンツ・スクランブルシステムでは、ＤＶＤ－ＲＯＭ(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー（復号鍵）が、ライセンスを受けたＤＶＤプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたＤＶＤプレーヤに対して与えられる。従って、ライセンスを受けたＤＶＤプレーヤでは、与えられたキーを利用して、ＤＶＤ－ＲＯＭに記録された暗号化データを復号することにより、ＤＶＤ－ＲＯＭから画像や音声を再生することができる。

【０００７】一方、ライセンスを受けていないＤＶＤプレーヤは、暗号化されたデータを復号するためのキーを有していないために、ＤＶＤ－ＲＯＭに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤは、ディジタルデータを記録したＤＶＤ－ＲＯＭの再生を行なえないことになり、不正コピーが防止されるようになっている。

【０００８】しかしながら、ＤＶＤ－ＲＯＭで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ＲＯＭメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、ＲＡＭメディアという）への適用については考慮されていない。

【０００９】即ち、ＲＯＭメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、ＲＡＭメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【００１０】そこで、本出願人は、先の特許出願、特願平１１－２２４４６１号公報（特願平１０－２５３１０号）において、個々の記録媒体を識別する為の情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

【００１１】この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

【００１２】ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

【００１３】

【発明が解決しようとする課題】ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、１つの機器で記録された媒体を他の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

【００１４】しかし、この方式においては、攻撃者が１つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

【００１５】上記問題を解決する構成として、本出願人は、各情報記録再生装置をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信

回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うようにすることにより、正当な（秘密が露呈していない装置に）対して少ないメッセージ量でマスターキーもしくはメディアキーを伝送できる構成を、先に提案し、すでに特許出願（特願平２０００－１０５３２８）している。具体的には、記録媒体への記録もしくは記録媒体からの再生に必要な鍵を生成するために必要となるキー、例えばｎ分木の各葉（リーフ）を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、更新ノードキーを正当な機器のみが有するリーフキー、ノードキーで復号可能な態様で暗号化処理した情報を含むキー更新ブロック（ＫＲＢ）を各情報記録再生装置に配信し、キー更新ブロック（ＫＲＢ）を受信した各情報記録再生装置のＫＲＢ復号処理により、各装置が記録もしくは記録媒体からの再生に必要な鍵を取得可能とした構成である。

【００１６】上記構成は、特定のシステム（記録再生装置グループ）の中のある装置が攻撃者の攻撃を受けて、その秘密であるデバイスキーが露呈したことが発覚した場合、それ以降に製造する記録媒体においては、秘密が露呈した記録再生装置をシステムから排除する、すなわち、排除されていない装置との記録再生の互換性をとれなくすることができるという特徴を持つ。

【００１７】しかし、この構成では、秘密が露呈した機器をシステムから排除できるのは、それが発覚した以降に製造される記録媒体においてのみであり、それ以前に製造された記録媒体においては、実際にデータを記録するのが上記の発覚時点以降だとしても、記録されたデータを、露呈した鍵で復号することができてしまう、すなわち、排除すべき装置を実際に排除できる場合が少ないという課題がある。

【００１８】本発明は、上記課題を解決することを目的とするものであり、秘密が露呈したことが発覚した以後、それ以前に製造された記録媒体でも、記録されたデータを露呈した鍵で復号できないようにすることを可能とし、より有効なコンテンツ暗号化を可能とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体を提供するものである。より、具体的には、記録媒体ごとにただひとつのメディアキーを設定するのではなく、複数のメディアキーを設定できるようにした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

【００１９】

【課題を解決するための手段】本発明の第１の側面は、記録媒体に情報を記録する情報記録装置において、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーを格納し、前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成される キー更新ブロック（ＫＲＢ）を格納するメモリ手段と、前記情報記録装置に内蔵した前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロック（ＫＲＢ）の復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に対する格納データの暗号化処理を実行する暗号処理手段と、を有し、前記暗号処理手段は、前記記録媒体に対するコンテンツの暗号化および格納処理において、記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報記録装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）中から利用可能な最新のキー更新ブロック（ＫＲＢ）を検出して、検出した利用可能な最新のキー更新ブロック（ＫＲＢ）の復号処理によって得られる暗号処理用キーを用いて記録媒体に対する格納データの暗号化処理を実行する構成を有することを特徴とする情報記録装置にある。

【００２０】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理用キーは、複数の情報記録装置に共通なマスターキー、情報記録装置に固有のデバイスキー、記録媒体に固有に設定されるメディアキーのいずれかであることを特徴とする。

【００２１】さらに、本発明の情報記録装置の一実施態様において、記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報記録装置自身の有するキー更新ブロック（ＫＲＢ）中の利用可能な最新のキー更新ブロック（ＫＲＢ）が、情報記録装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）であり、該最新のキー更新ブロック（ＫＲＢ）が記録媒体に未格納である場合において、記録媒体に対する前記最新のキー更新ブロック（ＫＲＢ）の書き込み処理を実行する構成を有することを特徴とする。

【００２２】さらに、本発明の情報記録装置の一実施態様において、記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報記録装置自身の有するキー更新ブロック（ＫＲＢ）中の利用可能な最新のキー更新ブロック（ＫＲＢ）が、記録媒体に格納したキー更新ブロック（ＫＲＢ）であり、該最新のキー更新ブロック（ＫＲＢ）が情報記録装置自身のメモリに未格納である場合において、情報記録装置自身のメモリに対する前記最新のキー更新ブロック（ＫＲＢ）の書き込み処理を実行する構成を有することを特徴とする。

【００２３】さらに、本発明の情報記録装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、前記暗号処理用キー更新処理に際して、更新ノードキーを下位階層のノードキーまたはリーフキーの少

なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を暗号処理用キー提供対象リーフの情報記録装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した暗号処理用キーを受領し、キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号処理用キーを算出する構成を有することを特徴とする。

【００２４】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする。

【００２５】さらに、本発明の第２の側面は、記録媒体から情報を再生する情報再生装置において、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーを格納し、前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成される木一更新ブロック（ＫＲＢ）を格納するメモリ手段と、前記情報再生装置に内蔵した前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロック（ＫＲＢ）の復号処理を実行して、前記記録媒体に格納された暗号データの復号処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に格納された暗号データの復号処理を実行する暗号処理手段と、を有し、前記暗号処理手段は、前記記録媒体に格納された暗号データの復号処理において、記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報再生装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック（ＫＲＢ）を検出して、検出したキー更新ブロック（ＫＲＢ）の復号処理によって得られる暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行する構成を有することを特徴とする情報再生装置にある。

【００２６】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理用キーは、複数の情報再生装置に共通なマスターキー、情報再生装置に固有のデバイスキー、記録媒体に固有に設定されるメディアキーのいずれかであることを特徴とする。

【００２７】さらに、本発明の情報再生装置の一実施態様において、記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報再生装置自身の有するキー更新ブロック（ＫＲＢ）中の利用可能な最新のキー更新ブロック（ＫＲＢ）が、記録媒体に格納したキー更新ブロック（ＫＲＢ）であり、該最新のキー更新ブロック（ＫＲＢ）が情報再生装置自身のメモリに未格納である場合において、情報再生装置自身のメモリに対する前記最新のキー更新ブロック（ＫＲＢ）の書き込み処理を実行する構成を有することを特徴とする。

【００２８】さらに、本発明の情報再生装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、前記暗号処理用キー更新処理に際して、更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を暗号処理用キー提供対象リーフの情報再生装置に配布する構成であり、前記情報再生装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した暗号処理用キーを受領し、キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号処理用キーを算出する構成を有することを特徴とする。

【００２９】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理用キーは、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする。

【００３０】さらに、本発明の第３の側面は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録装置における情報記録方法であり、記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報記録装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）中から利用可能な最新のキー更新ブロック（ＫＲＢ）を検出するＫＲＢ検出ステップと、前記ＫＲＢ検出ステップにおいて、検出された利用可能な最新のキー更新ブロック（ＫＲＢ）について、前記情報記録装置に内蔵したノードキーまたはリーフキーの少なくともいずれかを用いてキー更新ブロック（ＫＲＢ）の復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行するＫＲＢ復号処理ステップと、前記ＫＲＢ復号処理ステップにおいて、算出された暗号処理用キーを用いて前記記録媒体に対する記録データの暗号化を行ない記録媒体に格納するステップと、をもつことを特徴とする情報記録方法にある。

【００３１】さらに、本発明の情報記録方法の一実施態様において、前記ＫＲＢ検出ステップにおいて、検出した利用可能な最新のキー更新ブロック（ＫＲＢ）が、情報記録装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）であり、該最新のキー更新ブロック（ＫＲＢ）が記録媒体に未格納である場合において、記録媒体に対する前記最新のキー更新ブロック（ＫＲＢ）の書き込み処理を実行することを特徴とする。

【００３２】さらに、本発明の情報記録方法の一実施態様において、前記ＫＲＢ検出ステップにおいて、検出した利用可能な最新のキー更新ブロック（ＫＲＢ）が、記

録媒体に格納したキー更新ブロック（ＫＲＢ）であり、該最新のキー更新ブロック（ＫＲＢ）が情報記録装置自身のメモリに未格納である場合において、情報記録装置自身のメモリに対する前記最新のキー更新ブロック（ＫＲＢ）の書き込み処理を実行することを特徴とする。

【００３３】さらに、本発明の第４の側面は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を行なう情報再生装置における情報再生方法であり、記録媒体に格納され、再生対象となるコンテシツの暗号処理用キーのバージョン情報を取得するステップと、記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報再生装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック（ＫＲＢ）を検出する検出ステップと、前記検出ステップにおいて検出したキー更新ブロック（ＫＲＢ）の復号処理によって暗号処理用キーを生成するステップと、生成した暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行するステップと、をなることを特徴とする情報再生方法にある。

【００３４】さらに、本発明の情報再生方法の一実施態様において、前記ＫＲＢ検出ステップにおいて、検出した利用可能な最新のキー更新ブロック（ＫＲＢ）が、記録媒体に格納したキー更新ブロック（ＫＲＢ）であり、該最新のキー更新ブロック（ＫＲＢ）が情報再生装置自身のメモリに未格納である場合において、情報再生装置自身のメモリに対する前記最新のキー更新ブロック（ＫＲＢ）の書き込み処理を実行することを特徴とする。

【００３５】さらに、本発明の第５の側面は、情報を記録可能な情報記録媒体であって、複数の異なる情報記録装置または情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録または再生装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を、異なる構成を持つ複数のキー更新ブロック（ＫＲＢ）として、格納したことを特徴とする情報記録媒体にある。

【００３６】さらに、本発明の情報記録媒体の一実施態様において、前記複数のキー更新ブロック（ＫＲＢ）の各々は、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする。

【００３７】さらに、本発明の第６の側面は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録装置における情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報記録装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）中から利用可能な最新のキー更新ブロック（ＫＲＢ）を検出するＫＲＢ検出ステップと、前記ＫＲＢ検出ステップにおいて、検出された利用可能な最新のキー更新ブロック（ＫＲＢ）について、前記情報記録装置に内蔵したノードキーまたはリーフキーの少なくともいずれかを用いてキー更新ブロック（ＫＲＢ）の復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行するＫＲＢ復号処理ステップと、前記ＫＲＢ復号処理ステップにおいて、算出された暗号処理用キーを用いて前記記録媒体に対する記録データの暗号化を行なう記録媒体に格納するステップと、をなすことを特徴とするプログラム提供媒体にある。

【００３８】さらに、本発明の第７の側面は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を行なう情報再生装置における情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、記録媒体に格納され、再生対象となるコンテンツの暗号処理用キーのバージョン情報を取得するステップと、記録媒体に格納されたキー更新ブロック（ＫＲＢ）、および情報再生装置自身のメモリに格納したキー更新ブロック（ＫＲＢ）中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック（ＫＲＢ）を検出する検出ステップと、前記検出ステップにおいて検出したキー更新ブロック（ＫＲＢ）の復号処理によって暗号処理用キーを生成するステップと、生成した暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行するステップと、をなすことを特徴とするプログラム提供媒体にある。

【００３９】

【作用】本発明の構成においては、ツリー（木）構造の階層的鍵配信方式を用いることにより、キー更新に必要な配信メッセージ量を小さく押さえている。すなわち、各機器をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う。

【００４０】また、本発明では、前述の課題を解決するために、記録媒体ごとにただひとつのメディアキーを設定するのではなく、複数のメディアキーを設定できるようにする。すなわち、記録媒体が製造されて市場に出ま

わった後も、より新しいメディアキーを算出するためのキー更新ブロック（ＫＲＢ：Key Renewal Block）を記録再生装置が記録媒体に書きこめるようにする。データを記録媒体に記録する際には、記録再生装置は、記録媒体上のキー更新ブロック（ＫＲＢ：Key Renewal Block）と、自身が格納するＫＲＢのうち最新のものを用いてメディアキーを算出してデータの暗号化に使用し、またその最新のＫＲＢが記録媒体上にはなく自身が格納しているものであれば、それを記録媒体に格納するようにする。

【００４１】さらに記録再生装置は、記録媒体にアクセスする際に記録媒体上の全ＫＲＢのバージョンを調べ、その中の最新のものが、自身が格納するものより新しければ、これを用いて自身が格納するＫＲＢを最新のものに更新する。これらの処理によって、記録再生装置にはどんどん新しいＫＲＢが格納され、またデータが記録される際には、その時点で記録再生装置と記録媒体が格納する最新のＫＲＢにより算出されるメディアキーを用いてデータが暗号化されて記録されるから、たとえ記録媒体が製造されたのがとても古く、あらかじめ記録媒体に格納されているＫＲＢが古いものであったとしても、データが記録される際には新しいＫＲＢが使われる可能性が高いので、そのデータの安全性をより高く守ることが可能となる。

【００４２】なお、本発明の第６、第７の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００４３】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００４４】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００４５】

【発明の実施の形態】【システム構成】図１は、本発明を適用した記録再生装置１００の一実施例構成を示すブロック図である。記録再生装置１００は、入出力Ｉ／Ｆ（Interface）１２０、ＭＰＥＧ（Moving Picture Experts Group）コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えた入出力Ｉ／Ｆ（Interface）１４０、暗号処理手段１５０、ＲＯＭ（Read Only Memory）１６０、ＣＰＵ（Central Processing Unit）１７０、メモリ１８０、記録媒体１９５の記録媒体インタフェース（Ｉ／Ｆ）１９０を有し、これらはバス１１０によって相互に接続されている。

【００４６】入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するディジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のディジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック１３０は、バス１１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ１４０から供給されるディジタル信号をＭＰＥＧエンコードしてバス１１０上に出力する。入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ（Analog Digital）変換することで、ディジタル信号として、ＭＰＥＧコーデック１３０に出力するとともに、ＭＰＥＧコーデック１３０からのディジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ（Digital Analog）変換することで、アナログ信号として、外部に出力する。

【００４７】暗号処理手段１５０は、例えば、１チップのＬＳＩ（Large Scale IntegratedCurcuit）で構成され、バス１１０を介して供給されるコンテンツとしてのディジタル信号を暗号化し、または復号し、バス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【００４８】ＲＯＭ１６０は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。ＣＰＵ１７０は、メモリ１８０に記憶されたプログラムを実行することで、ＭＰＥＧコーデック１３０や暗号処理手段１５０等を制御する。メモリ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログラムや、ＣＰＵ１７０の動作上必要なデータを記憶する。記録媒体インタフェース１９０は、デジタルデータを記録再生可能な記録媒体１９５を駆動することにより、記録媒体１９５からディジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるディジタルデータを、記録媒体１９５に供給して記録させる。また、プログラムをＲＯＭ１６０に、デバイスキーをメモリ１８０に記憶する構成としてもよい。

【００４９】記録媒体１９５は、例えば、ＤＶＤ、ＣＤ

等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のディジタルデータの記憶可能な媒体であり、本実施の形態では、記録媒体インタフェース１９０に対して着脱可能な構成であるとする。但し、記録媒体１９５は、記録再生装置１００に内蔵する構成としてもよい。

【００５０】［データ記録処理およびデータ再生処理］次に、図１の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理について、図２および図３のフローチャートを参照して説明する。外部からのディジタル信号のコンテンツを、記録媒体１９５に記録する場合においては、図２（Ａ）のフローチャートにしたがった記録処理が行われる。即ち、ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ２０１において、入出力Ｉ／Ｆ１２０は、供給されるディジタルコンテンツを受信し、バス１１０を介して、暗号処理手段１５０に出力する。

【００５１】暗号処理手段１５０は、ステップＳ２０２において、受信したディジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス１１０を介して、記録媒体Ｉ／Ｆ１９０に出力する。暗号化コンテンツは、記録媒体Ｉ／Ｆ１９０を介して記録媒体１９５に記録（Ｓ２０３）され、記録処理を終了する。

【００５２】なお、IEEE1394シリアルバスを介して接続した装置相互間で、ディジタルコンテンツを伝送するときの、ディジタルコンテンツを保護するための規格として、５ＣＤＴＣＰ(Five Company Digital Transmission Content Protection)（以下、適宜、ＤＴＣＰという）が定められているが、このＤＴＣＰでは、コピーフリーでないディジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、ディジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたディジタルコンテンツ（暗号化コンテンツ）を復号するようになっている。

【００５３】このＤＴＣＰに規格に基づくデータ送受信においては、データ受信側の入出力Ｉ／Ｆ１２０は、ステップＳ２０１で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、ＤＴＣＰに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段１５０に出力する。

【００５４】ＤＴＣＰによるディジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたディジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたディジタルコンテンツを、そこに含まれるキーを用いて復号する。

【００５５】なお、ＤＴＣＰによれば、正確には、キーの初期値と、ディジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含められる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、ＤＴＣＰについては、例えば、http://www.dtcp.comのURL(Uniform Resource Locator)で特定されるＷｅｂページにおいて、インフォメイショナルバージョン(Informational Version)の取得が可能である。

【００５６】次に、外部からのアナログ信号のコンテンツを、記録媒体１９５に記録する場合の処理について、図２（Ｂ）のフローチャートに従って説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ２２１において、そのアナログコンテンツを受信し、ステップＳ２２２に進み、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ変換して、ディジタル信号のコンテンツ（ディジタルコンテンツ）とする。

【００５７】このディジタルコンテンツは、ＭＰＥＧコーデック１３０に供給され、ステップＳ２２３において、ＭＰＥＧエンコード、すなわちＭＰＥＧ圧縮による符号化処理が実行され、バス１１０を介して、暗号処理手段１５０に供給される。

【００５８】以下、ステップＳ２２４、Ｓ２２５において、図２（Ａ）のステップＳ２０２、Ｓ２０３における処理と同様の処理が行われる。すなわち、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

【００５９】次に、記録媒体１９５に記録されたコンテンツを再生して、ディジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図３のフローに従って説明する。ディジタルコンテンツとして外部に出力する処理は図３（Ａ）のフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ステップＳ３０１において、記録媒体Ｉ／Ｆ１９０によって、記録媒体１９５に記録された暗号化コンテンツが読み出され、バス１１０を介して、暗号処理手段１５０に出力される。

【００６０】暗号処理手段１５０では、ステップＳ３０２において、記録媒体Ｉ／Ｆ１９０から供給される暗号

化コンテンツが復号処理され、復号データがバス１１０を介して、入出力Ｉ／Ｆ１２０に供給される。ステップＳ３０３において、入出力Ｉ／Ｆ１２０はディジタルコンテンツを、外部に出力し、再生処理を終了する。

【００６１】なお、入出力Ｉ／Ｆ１２０は、ステップＳ３０３で、ＩＥＥＥ１３９４シリアルバスを介してディジタルコンテンツを出力する場合には、ＤＴＣＰの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、ディジタルコンテンツを暗号化して伝送する。

【００６２】記録媒体１９５に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図３（Ｂ）のフローチャートに従った再生処理が行われる。

【００６３】即ち、ステップＳ３２１、Ｓ３２２において、図３（Ａ）のステップＳ３０１、Ｓ３０２における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段１５０において得られた復号されたディジタルコンテンツは、バス１１０を介して、ＭＰＥＧコーデック１３０に供給される。

【００６４】ＭＰＥＧコーデック１３０では、ステップＳ３２３において、ディジタルコンテンツがＭＰＥＧデコード、すなわち伸長処理が実行され、入出力Ｉ／Ｆ１４０に供給される。入出力Ｉ／Ｆ１４０は、ステップＳ３２４において、ＭＰＥＧコーデック１３０でＭＰＥＧデコードされたディジタルコンテンツを、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ変換して、アナログコンテンツとする。そして、ステップＳ３２５に進み、入出力Ｉ／Ｆ１４０は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

【００６５】〔ｷｰ配信構成としてのツリー（木）構造について〕次に、図１に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なキー、例えばメディアキーを、各機器に配布する構成について説明する。図４は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図４の最下段に示すナンバ０～１５が個々の記録再生装置である。すなわち図４に示す木（ツリー）構造の各葉（リーフ：ｌｅａｆ）がそれぞれの記録再生装置に相当する。

【００６６】各デバイス０～１５は、製造時（出荷時）に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）およびあらリーフのリーフキーを自身で格納する。図４の最下段に示すＫ０００～Ｋ１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲから、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

【００６７】図４に示すツリー構成において、例えばデバイス０はリーフキーＫ０００２、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図４のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各節において異なる段数構成を持つことが可能である。

【００６８】また、図４のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばＤＶＤ、ＣＤ、ＭＤ、メモリスティック（商標）等を使用する様々なタイプの記録再生部が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図４に示すキー配布構成が適用されている。

【００６９】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図４の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して送付するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図４の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図４のツリー中に複数存在する。

【００７０】なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【００７１】このツリー構造において、図４から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス０，１，２，３のみに提供することが可能となる。たとえば、共通に保有するノードキーＫ００自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみが共通のマスターキーの設定が可能である。また、新たなマスターキーＫmaster

21

をノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Ｋmaster）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて候有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Ｋmaster）を解いてマスターキー：Ｋmasterを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータをあらわす。

【００７２】また、ある時点の世代：ｔにおいて、デバイス３の所有する鍵：Ｋ００１，Ｋ００１，Ｋ００，Ｋ００，ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１，Ｋ００，Ｋ００，ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）００，Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

【００７３】更新キーの配布処理について説明する。キーの更新は、例えば、図５（Ａ）に示すキー更新ブロック（ＫＲＢ：Key Renewal Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。

【００７４】図５（Ａ）に示すキー更新ブロック（ＫＲＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なマスター暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図５（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図５（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）

22

０、図５（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイス０，１はノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイス０，１は、図５（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００、を取得し、以下、図５（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図５（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）Ｒを得ることができる。なお、図５（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【００７６】図４に示すツリー構造の上位段のノードキー：Ｋ（ｔ）０，Ｋ（ｔ）Ｒの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図５（Ｂ）のキー更新ブロック（ＫＲＢ：Key Renewal Block）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【００７７】図５（Ｂ）に示すＫＲＢは、例えば特定のグループの情報記録装置において共有する新たなマスターキー、情報記録装置固有のデバイスキー、あるいは記録媒体に固有のメディアキーを配布する場合に利用可能である。具体例として、図４に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のマスターキーＫ（ｔ）masterが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新マスターキー：Ｋ（ｔ）masterを暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｔ）master）を図５（Ｂ）に示すＫＲＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。メディアキーについても同様である。

【００７８】すなわち、デバイス０，１，２はＫＲＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのマスターキー：Ｋ（ｔ）masterやメディアキー：Ｋ（ｔ）mediaを得ることが可能になる。

【００７９】以上をまとめると、各デバイスでの処理は、以下のように説明できる。

１．各デバイスはそれぞれ、ＫＲＢのインデックス（Index）部を見て、ＫＲＢで送られる木の構造を知る。

２．ＫＲＢによって更新されていない（生きている）ノードキーのうち最上位の鍵（この例では、デバイス０，１ならＫ０００、デバイス２ならＫ００１０）を用いて暗号文を解くことによって、そのノードの親のノードの更新されたノードキーを得る。

３．更新されたノードキーを用いて暗号文を解くことに

よって、そのノードの親のノードの更新されたノードキーを得る。

4．これを繰り返して、ＫＲＢの最上位のノードの更新されたノードキーを得る。

【００８０】なお、ＫＲＢの世代（Generation）は、そのＫＲＢのバージョンを表し、たとえば新しいものは値を大きくしておくなど、その値を比較することによってＫＲＢの新旧の比較が行えるようになっている。また、Ｋ（ｔ）０，Ｋ（ｔ）Ｒの更新が不要の場合には、図５（Ｂ）のＫＲＢ（Key Renewal Block）を用いることで、Ｋ（ｔ）００をデバイス０，１，２で共有することができる。すなわち、デバイス０，１，２，３がある記録媒体を用いるひとつのグループを形成するとき、Ｋ（ｔ）００を用いて伝送したメディアキーを用いて記録データを暗号化することにより、デバイス４など、その他のグループの機器からはアクセスされないデータとすることが可能となる。具体的に、たとえば図５（Ｂ）を用いてデバイス０，１，２はＫ（ｔ）００を共有するが、このＫＲＢを格納した記録媒体に、ｔ時点でのメディアキーＫ（ｔ）mediaを暗号化して格納しておく。デバイス０，１，２はＫＲＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号し、ｔ時点でのメディアキーＫ（ｔ）mediaを得る。

【００８１】［ＫＲＢを使用したメディアキーの取得］図６に、本出願人の先の特許出願である特願平２０００－１０５３２８で提案したｔ時点でのメディアキーＫ（ｔ）mediaを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のメディアキーＫ（ｔ）mediaを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）media）と図５（Ｂ）に示すＫＲＢとを記録媒体を介して受領したデバイス２の処理を示す。

【００８２】図４に示すように、ある記録再生システムには、点線で囲まれた、デバイス０，１，２，３の４つの装置が含まれるとする。図６は、デバイス３がリボークされたときに、記録媒体どとに割り当てられるメディアキーを使用する場合に、記録再生装置（デバイス２）が記録媒体上のコンテンツを暗号化もしくは復号するために必要なメディアキーを、記録媒体に格納されているＫＲＢ（Key RenewalBlock）と記録再生装置が記憶するデバイスキーを用いて求める際の処理を表している。

【００８３】デバイス２のメモリには、自分にのみ割り当てられたリーフキーＫ＿００１０と、それから木のルートまでの各ノードＲ００１，００，０，Ｒのノードキー（それぞれ、Ｋ＿００１，Ｋ＿００，Ｋ＿０，Ｋ＿Ｒ）が安全に格納されている。デバイス２は、図６の記録媒体に格納されているＫＲＢのうち、インデックス（Index）が００１０の暗号文を自分の持つリーフキーＫ＿００１０で復号してノードＲ００１のノードキーＫ（ｔ）＿００１を計算し、次にそれを用いてインデックス（Index）が００１の暗号文を復号してノードＲ００のノードキーＫ（ｔ）＿００を計算し、最後にそれを用いて暗号文を復号してメディアキーＫ（ｔ）＿mediaを計算する。このようにして計算され、取得されたメディアキーを用いたデータの暗号化処理、復号処理順様について、以下、説明する。

【００８４】［メディアキーを用いた暗号化処理、復号処理］図７の処理ブロック図に従って、暗号処理手段１５０が実行するデータの暗号化処理および記録媒体に対する記録処理の一例について説明する。

【００８５】記録再生装置７００は自身の上述したＫＲＢに基づく算出処理によってメディアキーを取得する。

【００８６】次に、記録再生装置７００は例えば光ディスクである記録媒体７０２に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていれば、ディスクＩＤ（Disc ID）を読出し、記録されていなければ、暗号処理手段１５０においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクＩＤ（Disc ID）１７０１を生成し、ディスクに記録する。ディスクＩＤ（Disc ID）はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【００８７】記録再生器７００は、次にメディアキー７０１とディスクＩＤを用いて、ディスク固有キー（Disc Unique Key）を生成する。ディスク固有キー（Disc UnqueKey）の具体的な生成方法としては、図８に示すように、ブロック暗号関数を用いたハッシュ関数にメディアキーとディスクＩＤ（Disc ID）を入力して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、メディアキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する例２の方法が適用できる。

【００８８】次に、記録どとの固有鍵であるタイトルキー（Title Key）を暗号処理手段１５０（図１参照）においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成し、ディスク７０２に記録する。

【００８９】次にディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤ、あるいは、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイス固有キー、いずれかの組合せから、タイトル固有キー（Title Unique Key）を生成する。

【００９０】このタイトル固有キー（Title Unique Key）生成の具体的な方法は、図９に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー（Title Key）とディスク固有キー（Disc Unique Key）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を入力して得

られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、メディアキーとディスクＩＤ（Disc ID）とデバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをタイトル固有キー（Title Unique Key）として使用する例２の方法が適用できる。なお、再生機器制限とは、記録媒体に格納されたコンテンツデータを制限された特定の再生機器においてのみ再生可能とすることを意味する。

【００９１】なお、上記の説明では、メディアキーとディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデバイスＩＤ、もしくはタイトルキー（Title Key）とデバイス固有キーからタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてメディアキーとディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、デバイスＩＤもしくはデバイス固有キーから直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、メディアキー（Media Key）とディスクＩＤ（Disc ID）と、デバイスＩＤもしくはデバイス固有キーからタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

【００９２】さらに、図７を用いて、その後の処理を説明する。被暗号化データとして入力されるブロックデータの先頭の第１～４バイトが分離されて出力されるブロックシード（Block Seed）と、先に生成したタイトル固有キー（Title Unique Key）とから、そのブロックのデータを暗号化する鍵であるブロック・キー（Block Key）が生成される。

【００９３】ブロック・キー（Block Key）の生成方法の例を図１０に示す。図１０では、いずれも３２ビットのブロック・シード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する例を２つ示している。

【００９４】上段に示す例１は、鍵長６４ビット、入出力がそれぞれ４ビットの暗号関数を使用している。タイトル固有キー（Title Unique Key）をこの暗号関数の鍵とし、ブロックシード（Block Seed）と３２ビットの定数（コンスタント）を連結した値を入力して暗号化した結果をブロックキー（Block Key）としている。

【００９５】例２は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー（Title Unique Key）とブロックシード（Block Seed）を連結した値をＳＨＡ－１に入力し、その１６０ビットの出力を、たとえば下位６４ビットのみ使用するなど、６４ビットに縮約したものをブロックキー（Block Key）としている。

【００９６】なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロックごとにメディアキーとディスクＩＤ（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）と、デバイスＩＤ、もしくはデバイス固有キーを用いてブロックキー（Block Key）を生成してもよい。

【００９７】ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図７の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第１～mバイト（たとえばm＝８バイト）は分離（セレクタ１６０８）されて暗号化対象とせず、m＋１バイト目から最終データまでを暗号化する。なお、暗号化されないmバイト中にはブロック・シードとしての第１～４バイトも含まれる。セレクタにより分離された第m＋１バイト以降のブロックデータは、暗号処理手段１５０に予め設定された暗号化アルゴリズムに従って暗号化される。暗号化アルゴリズムとしては、たとえばFIPS46-2で規定されるＤＥＳ（Data Encryption Standard）を用いることができる。

【００９８】以上の処理により、コンテンツはブロック単位で、世代管理されたメディアキー、ブロック・シード等に基づいて生成されるブロックキーで暗号化が施されて記録媒体に格納される。

【００９９】記録媒体に格納された暗号化コンテンツデータの復号および再生処理を説明するブロック図１１に示す。

【０１００】再生処理においては、図７～図１０を用いて説明した暗号化および記録処理と同様、メディアキーとディスクＩＤからディスク固有キーを生成し、ディスク固有キーと、タイトルキーからタイトル固有キーを生成し、さらにタイトルキーと記録媒体から読み取られるブロックシードとから、ブロックキーを生成して、ブロックキーを復号キーとして用い、記録媒体７０２から読み取られるブロック単位の暗号化データの復号処理を実行する。

【０１０１】上述のように、コンテンツデータの記録媒体に対する記録時の暗号化処理、および記録媒体からの再生時の復号処理においては、ＫＲＢに基づいてメディアキーを算出し、その後算出したメディアキーと他の識別子等に基づいて、コンテンツの暗号化処理用の鍵、または復号処理用の鍵を生成する。

【０１０２】なお、上述した例では、メディアキーを用いてコンテンツデータの暗号化処理、および復号処理に用いるキーを生成する構成を説明したが、メディアキー

ではなく、複数の記録再生装置に共通のマスターキー、あるいは記録再生器固有のデバイスキーをＫＲＢから取得して、これらに基づいてコンテンツデータの暗号化処理、および復号処理に用いるキーを生成する構成としてもよい。さらに、ＫＲＢから取得されるメディアキー、マスターキー、あるいはデバイスキー自体をコンテンツデータの暗号化処理、および復号処理に用いるキーとして適用することも可能である。

【０１０３】上述のように、キー更新ブロック（ＫＲＢ）を用いることにより、正当なライセンスを受けたデバイスに対してのみ安全に更新キーを提供し、提供したキーによって記録媒体に対するコンテンツ暗号化処理、または記録媒体から読み出したコンテンツの復号処理に用いるキーの生成が可能となる。上述の構成では、例えば１つの記録媒体にただ１つのキー更新ブロック（ＫＲＢ）を格納し、これを利用して更新キーの取得を行なう例を説明したが、さらに、複数のキー更新ブロック（ＫＲＢ）を格納した構成例について、以下説明する。この場合、後段で詳細に説明するが、記録媒体上の記録暗号化コンテンツデータの各々を、複数のキー更新ブロック（ＫＲＢ）のいずれのＫＲＢから生成されるメディアキーを用いて暗号化されたのかが判別可能な情報を持つ構成とする。

【０１０４】また、記録媒体のみではなく、記録再生装置のメモリにＫＲＢを格納する構成としてもよい。記録再生装置のキー更新ブロック（ＫＲＢ）格納用の記憶手段は、書き換え可能な構成であり、記録再生装置は、記録媒体へのアクセス時、たとえば、記録媒体が記録再生装置に装着された際に、記録媒体上のＫＲＢを検索し、その中で一番バージョンが新しいものが、自身が格納するものよりも新しければ、これを用いて自身の格納するＫＲＢを更新する。

【０１０５】［ＫＲＢのフォーマット］図１２にキー更新ブロック（ＫＲＢ：Key Renewal Block）のフォーマット例を示す。バージョン１２０１は、キー更新ブロック（ＫＲＢ：Key Renewal Block）のバージョンを示す識別子である。デプスは、キー更新ブロック（ＫＲＢ：Key Renewal Block）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ１２０３は、キー更新ブロック（ＫＲＢ：Key Renewal Block）中のデータ部の位置を示すポインタであり、タグポインタ１２０４はタグ部の位置、署名ポインタ１２０５は署名の位置を示すポインタである。データ部１２０６は、例えば更新するノードキーを暗号化したデータを格納する。

【０１０６】タグ部１２０７は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図１３を用いて説明する。図１３では、データとして先に図５（Ａ）で説明したキー更新ブロック（ＫＲＢ）を送付する例を示している。この時のデータは、図１３の右の表に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キー－Ｋ（ｔ）Ｒが含まれているので、トップノードアドレスはＫＲとなる。

【０１０７】暗号化キーの最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図１３の左の階層ツリーに示す位置にある。ここで、次のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが０、ない場合は１が設定される。タグは（左（Ｌ）タグ，右（Ｒ）タグ）として設定される。最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左にはデータがあるので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図１３（ｃ）に示すデータ列、およびタグ列が構成される。

【０１０８】図１２に戻って、ＫＲＢフォーマットについてさらに説明する。署名（Signature）は、キー更新ブロック（ＫＲＢ）を発行した例えば鍵管理センタ、コンテンツプロバイダ、決済機関等が実行する電子署名である。ＫＲＢを受領したデバイスは署名検証によって正当なキー更新ブロック（ＫＲＢ）発行者が発行したキー更新ブロック（ＫＲＢ）であることを確認する。

【０１０９】［複数のキー更新ブロック（ＫＲＢ）を選択利用する構成］次に、記録媒体に複数のキー更新ブロック（ＫＲＢ）を格納する構成、さらに、記録再生装置のメモリに最新のＫＲＢを格納する処理、すなわち、記録再生装置側に格納したキー更新ブロック（ＫＲＢ）を更新する処理について、図１４のイメージ図および図１５のフローチャートを用いて説明する。

【０１１０】図１４の上段に示す（Ａ）は、記録再生機器に記録媒体が装着される以前の状態であり、記録再生装置１４１０に１つのキー更新ブロック（ＫＲＢ）１４１１が格納され、記録媒体１４２０には、２つのキー更新ブロック（ＫＲＢ）１４２１，１４２２が格納されている状態を示している。

【０１１１】記録再生装置１４１０に格納されたＫＲＢは、バージョン（Ｔ１）のキー更新ブロック（ＫＲＢ）１４１１であり、記録媒体１４２０に格納されたＫＲＢは、バージョン（Ｔ１）のキー更新ブロック（ＫＲＢ）１４２１、およびバージョン（Ｔ２）のキー更新ブロック（ＫＲＢ）１４２２である。ここでバージョンＴ２はバージョンＴ１より新しいものとする。

【０１１２】また、記録媒体１４２０には、バージョン（Ｔ１）のキー更新ブロック（ＫＲＢ）から生成されるメディアキーを用いて暗号化されたコンテンツ１４３１と、バージョン（Ｔ２）のキー更新ブロック（ＫＲＢ）から生成されるメディアキーを用いて暗号化されたコンテンツ１４３２が格納されている。

【０１１３】記録媒体１４２０が記録再生装置１４１０

に装着された際、記録再生装置は図１５のフローチャートに従って、自身の格納するキー更新ブロック（ＫＲＢ）の更新処理を行う。

【０１１４】図１５のステップＳ１５０１で、記録再生装置１４１０は、記録媒体１４２０に格納されているすべての一更新ブロック（ＫＲＢ）の世代情報（Generation）であるバージョンを読出し、その中で最新のものを見つける。図１４（Ａ）に示す例では、バージョン（Ｔ２）のキー更新ブロック（ＫＲＢ）１４２２が最新である。

【０１１５】ステップＳ１５０２において、記録再生装置１４１０は、記録再生装置内のメモリ（例えば図１のメモリ１８０）に格納しているキー更新ブロック（ＫＲＢ）と、ステップＳ１５０１で検出した記録媒体１４２０上の最新ＫＲＢ、すなわちバージョン（Ｔ２）のキー更新ブロック（ＫＲＢ）１４２２との新旧を比較する。

【０１１６】この比較において、記録媒体上から検出したＫＲＢの方が新しければステップＳ１５０３に進み、そうでなければステップＳ１５０３、Ｓ１５０４をスキップして処理を終了する。

【０１１７】図１４（Ａ）の例では、記録再生装置１４１０が格納しているのはバージョン（Ｔ１）のキー更新ブロック（ＫＲＢ）１４１１であり、これよりバージョン（Ｔ２）のキー更新ブロック（ＫＲＢ）１４２２の方が新しいので、ステップＳ１５０３に進む。

【０１１８】ステップＳ１５０３では、記録再生装置１４１０が保有しているリーフキー、ノードキーを用いて更新予定の最新のＫＲＢが復号可能か否かを判定する。すなわち、先の図４、５、６等で説明したように、自己の有するリーフキー、あるいはノードキーによりキー更新ブロック（ＫＲＢ）を順次復号し、世代の更新された世代情報：ｔの新バージョンのノードキー、例えばＫ（ｔ）００、あるいはルートキーＫ（ｔ）Ｒが取得可能か否かを判定する。この判定処理は、例えば図５に示すキー更新ブロック（ＫＲＢ）において、いずれかのインデックスに自己の有するリーフキー、ノードキーをそのまま適用して復号可能な暗号化キーが格納されているか否かを判定することによって行なわれる。

【０１１９】ステップＳ１５０３において、記録再生装置１４１０が保有しているリーフキー、ノードキーを用いて更新予定の最新のＫＲＢが復号可能であると判定された場合は、ステップＳ１５０４に進む。復号不可と判定された場合は、ステップＳ１５０４をスキップして処理を終了する。

【０１２０】ステップＳ１５０４では、ステップＳ１５０１で検出した記録媒体１４２０に格納された最新のＫＲＢを用いて、記録再生装置１４１０がメモリに格納しているバージョン（Ｔ１）のキー更新ブロック（ＫＲＢ）１４１１を更新する。この結果、図１４（Ｂ）に示すように、記録再生装置１４１０に格納されるＫＲＢがバージョン（Ｔ２）のキー更新ブロック（ＫＲＢ）１４１２に更新される。

【０１２１】次に、図１６および図１７のフローチャートを用いて、図１に示した記録再生装置が記録媒体にコンテンツデータを記録する処理を説明する。

【０１２２】図１６の上段に示す（Ａ）の記録再生装置１６１０は、バージョン（Ｔ２）のキー更新ブロック（ＫＲＢ）１６１１を格納しており、コンテンツを暗号化して記録媒体１６２０に記録しようとしている。

【０１２３】記録媒体１６２０には、バージョン（Ｔ１）のキー更新ブロック（ＫＲＢ）１６２１が記録されており、このキー更新ブロック（ＫＲＢ）１６２１から生成されたメディアキーに基づいて暗号化されたコンテンツ１６３１が記録されている。

【０１２４】図１７は、記録再生装置が記録媒体に対してコンテンツデータを記録する際の処理フローを示したものである。図１７のフローの各ステップについて説明する。

【０１２５】ステップＳ１７０１において、記録再生装置１６１０は自身が格納するバージョン（Ｔ２）のキー更新ブロック（ＫＲＢ）１６１１からメディアキーを生成する。

【０１２６】記録再生装置１６１０は、この記録媒体１６２０が装着されたときに、先に説明した図１５のキー更新ブロック（ＫＲＢ）更新処理を行っており、装置のメモリ内には装置および媒体上のキー更新ブロック（ＫＲＢ）のうちの最新のもの、ここではバージョンＴ２のキー更新ブロック（ＫＲＢ）が格納されている。

【０１２７】ステップＳ１７０２で、このメディアキーに基づいてコンテンツデータを暗号化する。この暗号化処理は、例えば先に図７を用いて説明した方法に従って実行される。その後、暗号化コンテンツデータは記録媒体１６２０に記録される。なお、暗号化コンテンツの記録媒体１６２０に対する格納処理の際に、そのコンテンツ暗号化に用いたメディアキーを取得したキー更新ブロック（ＫＲＢ）の世代情報としてのバージョン、この場合は、キー更新ブロック（ＫＲＢ）１６１１のバージョン（Ｔ２）を暗号化コンテンツに対応付けて記録媒体１６２０に記録する。この、キー更新ブロック（ＫＲＢ）の世代情報としてのバージョン情報は、具体的にはたとえば、図７に示すタイトルキー等のコンテンツの付加情報と同様、コンテンツデータに関連づけられた管理ファイルとして構成されるデータ管理ファイル中に記録されて記録媒体１６２０に格納される。

【０１２８】次に、ステップＳ１７０３において、記録再生装置１６１０は、メディアキーを生成するのに用いたと同じバージョンのキー更新ブロック（ＫＲＢ）が、記録媒体１６２０に格納されているかどうかを検査する。もし記録媒体１６７２０に格納されていれば、ステップＳ１７０４をスキップして処理を終了し、格納され

でいなければ、Ｓ１７０４に進む。

【０１２９】ステップＳ１７０４では、記録再生装置１６１０は記録媒体１６２０に、メディアキーを生成するのに用いたのと同じバージョンのキー更新ブロック（ＫＲＢ）、この場合は、バージョン（Ｔ２）のキー更新ブロック（ＫＲＢ）を記録し、コンテンツデータの記録処理を終了する。以上の処理により、図１６の（Ｂ）で示すように、記録媒体１６２０には、利用可能な最新のＫＲＢから取得されるメディアキーを用いて暗号化した暗号化コンテンツデータと、およびコンテンツ暗号処理に必要となるメディアキーを得るために必要となる最新のキー更新ブロック（ＫＲＢ）を記録媒体１６２０に記録することができる。

【０１３０】次に、上記のようにして、利用可能な最新のキー更新ブロック（ＫＲＢ）に基づいて得られるキーを利用して暗号化され、記録されたコンテンツデータを、記録媒体から記録再生装置が読み出す処理を、図１８のフローチャートを用いて説明する。

【０１３１】ステップＳ１８０１において、記録再生装置は、再生するコンテンツデータを暗号化したメディアキーを生成するキー更新ブロック（ＫＲＢ）の世代情報としてのバージョンを読み出す。記録媒体上の各コンテンツデータに対応するキー更新ブロック（ＫＲＢ）の世代情報としてのバージョンは、たとえば前述のデータ管理ファイルに書かれている。

【０１３２】ステップＳ１８０２で、記録再生装置は、記録媒体上に格納されている１以上のキー更新ブロック（ＫＲＢ）のうち、ステップＳ１８０１において読み出した世代情報としてのバージョンと同一のバージョンを持つものを検出し、そのキー更新ブロック（ＫＲＢ）を復号処理して、メディアキーを生成する。

【０１３３】次に、ステップＳ１８０３で、記録再生装置は、記録媒体からコンテンツデータを読み出し、Ｓ１８０２で生成したメディアキーに基づいてこれを復号して使用する。以上の処理により、記録媒体に格納されたコンテンツデータを再生することができる。

【０１３４】このように、本発明の情報記録再生装置では、複数の異なる世代、すなわちバージョンを持つキー更新ブロック（ＫＲＢ）を格納した記録媒体から最新のキー更新ブロック（ＫＲＢ）を取り出して、記録再生装置内のメモリに格納し、さらに、記録媒体に対するコンテンツ格納処理においては、記録再生装置内のメモリに格納されたＫＲＢ、および記録媒体に格納された複数のＫＲＢ中から、利用可能な最新のキー更新ブロック（ＫＲＢ）を検出して、その最新ＫＲＢから暗号処理用のキー、例えばメディアキーを取得して、取得した最新のメディアキーを用いてコンテンツの暗号化処理を実行して、記録媒体に格納し、コンテンツの暗号化に用いたメディアキーを取得したキー更新ブロック（ＫＲＢ）を新たに記録媒体に格納する構成とした。

【０１３５】このように複数のバージョンのＫＲＢを記録媒体に格納可能とするとともに、異なるＫＲＢから取得したメディアキーで暗号化したコンテンツを記録媒体に格納可能な構成とし、コンテンツを記録媒体に新たに記録する際には、その時点で記録再生装置と記録媒体が保有する最新のＫＲＢに基づいて算出されるメディアキーを用いてコンテンツの暗号化がなされるので、例えば記録媒体の製造時にコンテンツ暗号化に用いられた古いバージョンのＫＲＢが記録媒体に格納済みであっても、先に図４、図５を用いて説明したように、新たに鍵管理センタ、プロバイダ、決済機関等が実行するキー更新処理によって発行された新しいバージョンのＫＲＢを不正な機器をリボークして発行することにより、その後、記録媒体に格納される暗号化コンテンツは、正当な機器のみが取得可能な新しいバージョンのＫＲＢから取得されるメディアキーに基づいて暗号化されることになるので、リボークされた機器における復号、再生を排除することが可能となる。

【０１３６】【記録処理におけるコピー制御】さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

【０１３７】即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの（コピー可能）かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

【０１３８】そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図１の記録再生装置の処理について、図１９および図２０のフローチャートを参照して説明する。

【０１３９】まず、外部からのディジタル信号のコンテンツを、記録媒体に記録する場合においては、図１９（Ａ）のフローチャートにしたがった記録処理が行われる。図１９（Ａ）の処理について説明する。図１の記録再生器１００を例として説明する。ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ１９０１において、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを受信し、ステップＳ１９０２に進む。

【０１４０】ステップＳ１９０２では、入出力Ｉ／Ｆ１２０は、受信したディジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力Ｉ／Ｆ１２０が受信したコンテンツが暗号化されていない場合（例えば、上述のＤＴＣＰを使用せずに、平文のコンテンツが、入出力Ｉ／Ｆ１２０に供給された場合）には、そのコンテンツは、コピー可能であると判定され

る。

【０１４１】また、記録再生装置１００がＤＴＣＰに準拠している装置であるとし、ＤＴＣＰに従って処理を実行するものとする。ＤＴＣＰでは、コピー制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)が規定されている。ＥＭＩが００Ｂ（Ｂは、その前の値が２進数であることを表す）である場合は、コンテンツがコピーフリーのもの(Copy-freely)であることを表し、ＥＭＩが０１Ｂである場合には、コンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、ＥＭＩが１０Ｂである場合は、コンテンツが、１度だけコピーして良いもの(Copy-one-generation)であることを表し、ＥＭＩが１１Ｂである場合には、コンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。

【０１４２】記録再生装置１００の入出力Ｉ／Ｆ１２０に供給される信号にＥＭＩが含まれ、そのＥＭＩが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、ＥＭＩが、No-more-coplesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

【０１４３】ステップＳ１９０２において、コンテンツがコピー可能でないと判定された場合、ステップＳ１９０３～Ｓ１９０４をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体１０に記録されない。

【０１４４】また、ステップＳ１９０２において、コンテンツがコピー可能であると判定された場合、ステップＳ１９０３に進み、以下、ステップＳ１９０３～Ｓ１９０４において、図２（Ａ）のステップＳ２０２、Ｓ２０３における処理と同様の処理が行われる。すなわち、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

【０１４５】なお、ＥＭＩは、入出力Ｉ／Ｆ１２０に供給されるディジタル信号に含まれるものであり、ディジタルコンテンツが記録される場合には、そのディジタルコンテンツとともに、ＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（例えば、ＤＴＣＰにおけるembedded CCIなど）も記録される。

【０１４６】この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-coplesに変換されて記録される。

【０１４７】外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図１９（Ｂ）のフローチャートにしたがった記録処理が行われる。図１９（Ｂ）の処理について説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ１９

１１において、そのアナログコンテンツを受信し、ステップＳ１９１２に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

【０１４８】ここで、ステップＳ１９１２の判定処理は、例えば、入出力Ｉ／Ｆ１４０で受信した信号に、マクロビジョン(Macrovision)信号や、ＣＧＭＳ－Ａ(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、ＶＨＳ方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力Ｉ／Ｆ１４０で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

【０１４９】また、例えば、ＣＧＭＳ－Ａ信号は、ディジタル信号のコピー制御に用いられるＣＧＭＳ信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、１度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

【０１５０】従って、ＣＧＭＳ－Ａ信号が、入出力Ｉ／Ｆ１４０で受信した信号に含まれ、かつ、そのＣＧＭＳ－Ａ信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

【０１５１】さらに、例えば、マクロビジョン信号も、ＣＧＭＳ－Ａ信号も、入出力Ｉ／Ｆ４で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

【０１５２】ステップＳ１９１２において、アナログコンテンツがコピー可能でないと判定された場合、ステップＳ１９１３乃至Ｓ１９１６をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体１９５に記録されない。

【０１５３】また、ステップＳ１９１２において、アナログコンテンツがコピー可能であると判定された場合、ステップＳ１９１３に進み、以下、ステップＳ１９１３乃至Ｓ１９１６において、図２（Ｂ）のステップＳ２２乃至Ｓ２２５における処理と同様の処理が行われ、これにより、コンテンツがデジタル変換、ＭＰＥＧ符号化、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

【０１５４】なお、入出力Ｉ／Ｆ１４０で受信したアナログ信号に、ＣＧＭＳ－Ａ信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのＣＧＭＳ－Ａ信号も、記録媒体に記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-coplesに変換されて記録される。ただし、システムにおいてたとえ

ば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【０１５５】［再生処理におけるコピー制御］次に、記録媒体に記録されたコンテンツを再生して、ディジタルコンテンツとして外部に出力する場合においては、図２０（Ａ）のフローチャートにしたがった再生処理が行われる。図２０（Ａ）の処理について説明する。まず最初に、ステップＳ２００１、Ｓ２００２において、図３（Ａ）のステップＳ３０１、Ｓ３０２における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段１５０において復号処理がなされ、復号処理が実行されたディジタルコンテンツは、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給される。

【０１５６】入出力Ｉ／Ｆ１２０は、ステップＳ２００３において、そこに供給されるディジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（コピー制御情報）が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【０１５７】また、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩ等のコピー制御情報が含まれる場合、従って、コンテンツの記録時に、ＤＴＣＰの規格にしたがって、ＥＭＩが記録された場合には、そのＥＭＩ（記録されたＥＭＩ（Recorded EMI））が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。また、ＥＭＩが、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

【０１５８】なお、一般的には、記録されたＥＭＩが、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのＥＭＩは記録時にNo-more-copiesに変換され、また、Copy-neverのＥＭＩを持つディジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【０１５９】ステップＳ２００３において、コンテンツが、後でコピー可能なものであると判定された場合、ステップＳ２００４に進み、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを、外部に出力し、再生処理を終了する。

【０１６０】また、ステップＳ２００３において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップＳ２００５に進み、入出力Ｉ／Ｆ１２０は、例えば、ＤＴＣＰの規格等にしたがって、ディジタルコンテンツを、そのディジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【０１６１】即ち、例えば、上述のように、記録されたＥＭＩが、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩがCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【０１６２】このため、入出力Ｉ／Ｆ１２０は、ＤＴＣＰの規格にしたがい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、ＤＴＣＰの規格に準拠した装置である場合）には、ディジタルコンテンツを暗号化して、外部に出力する。

【０１６３】次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図２０（Ｂ）のフローチャートにしたがった再生処理が行われる。図２０（Ｂ）の処理について説明する。ステップＳ２０１１乃至Ｓ２０１４において、図３（Ｂ）のステップＳ３２１乃至Ｓ３２４における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、ＭＰＥＧデコード、Ｄ／Ａ変換が実行される。これにより得られるアナログコンテンツは、入出力Ｉ／Ｆ１４０で受信される。

【０１６４】入出力Ｉ／Ｆ１４０は、ステップＳ２０１５において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、記録されていたコンテンツにＥＭＩ等のコピー制御情報いっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【０１６５】また、コンテンツの記録時に、例えば、ＤＴＣＰの規格にしたがって、ＥＭＩ等のコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

【０１６６】また、ＥＭＩ等のコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ等のコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

【０１６７】さらに、例えば、入出力Ｉ／Ｆ１４０に供給されるコンテンツにＣＧＭＳ－Ａ信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにＣＧＭＳ－Ａ信号が記録された場合には、そのＣ

ＧＭＳ－Ａ信号が、Copy-Freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverであるときには、コンテンツは、後でコピー可能なものでないと判定される。

【０１６８】ステップＳ２０１５において、コンテンツが、後でコピー可能であると判定された場合、ステップＳ２０１６に進み、入出力Ｉ／Ｆ１４０は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

【０１６９】また、ステップＳ２０１５において、コンテンツが、後でコピー可能でないと判定された場合、ステップＳ２０１７に進み、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【０１７０】即ち、例えば、上述のように、記録されたＥＭＩ等のコピー制御情報が、No-more-coplesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-coplesに変換せずに記録するが、No-more-coplesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【０１７１】このため、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すＧＣＭＳ－Ａ信号を付加して、外部に出力する。また、例えば、記録されたＣＧＭＳ－Ａ信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力Ｉ／Ｆ４は、ＣＧＭＳ－Ａ信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

【０１７２】以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

【０１７３】［データ処理手段の構成］なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段１５０は暗号化／復号ＬＳＩとして構成することも可能であるが、汎用のコンピュータや、１チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや１チップのマイクロコンピュータ等にインストールされる。図２１は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【０１７４】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク２１０５やＲＯＭ２１０３に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体２１１０は、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体２１１０は、いわゆるパッケージソフトウエアとして提供することができる。

【０１７５】なお、プログラムは、上述したようなリムーバブル記録媒体２１１０からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、ＬＡＮ(Local AreaNetwork)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部２１０８で受信し、内蔵するハードディスク２１０５にインストールすることができる。

【０１７６】コンピュータは、ＣＰＵ(Central Processing Unit)２１０２を内蔵している。ＣＰＵ２１０２には、バス２１０１を介して、入出力インタフェース２１１１が接続されており、ＣＰＵ２１０２は、入出力インタフェース２１１０を介して、ユーザによって、キーボードやマウス等で構成される入力部２１０７が操作されることにより指令が入力されると、それにしたがって、ＲＯＭ(Read Only Memory)２１０３に格納されているプログラムを実行する。

【０１７７】あるいは、ＣＰＵ２１０２は、ハードディスク２１０５に格納されているプログラム、衛星若しくはネットワークから転送され、通信部２１０８で受信されてハードディスク２１０５にインストールされたプログラム、またはドライブ２１０９に装着されたリムーバブル記録媒体２１１０から読み出されてハードディスク２１０５にインストールされたプログラムを、ＲＡＭ(Random Access Memory)２１０４にロードして実行する。

【０１７８】これにより、ＣＰＵ２１０２は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、ＣＰＵ２１０２は、その処理結果を、必要に応じて、例えば、入出力インタフェース２１１１を介して、ＬＣＤ(Liquid CrySTal Display)やスピーカ等で構成される出力部２１０６から出力、あるいは、通信部２１０８から送信、さらには、ハードディスク２１０５に記録させる。

【０１７９】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あ

るいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【０１８０】また、プログラムは、１のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【０１８１】なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、１チップの暗号化／復号ＬＳＩで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図１に示すＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することも可能である。

【０１８２】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１８３】

【発明の効果】以上、説明したように、本発明の情報記録再生装置によれば、複数の異なる世代、バージョンを持つキー更新ブロック（ＫＲＢ）を記録媒体に格納可能とするとともに、最新のキー更新ブロック（ＫＲＢ）を取り出して、記録再生装置内のメモリに格納することを可能とした。さらに、記録媒体に対するコンテンツ格納処理においては、記録再生装置内のメモリに格納されたＫＲＢ、および記録媒体に格納された複数のＫＲＢ中から、利用可能な最新のキー更新ブロック（ＫＲＢ）を検出して、その最新ＫＲＢから暗号処理用のキー、例えばメディアキーを取得して、取得した最新のメディアキーを用いてコンテンツの暗号化処理を実行して、記録媒体に格納し、コンテンツの暗号化に用いた例えばメディアキーを取得したキー更新ブロック（ＫＲＢ）を新たに記録媒体に格納する構成とした。従って、コンテンツを記録媒体に新たに記録する際には、より新しいＫＲＢに基づいて算出されるメディアキーを用いた暗号化がなされる。

【０１８４】従って、例えば記録媒体の製造時にコンテンツ暗号化に用いられた古いバージョンのＫＲＢが記録媒体に格納済みであっても、より新しいＫＲＢに基づく暗号処理キーによるコンテンツ暗号化および格納が可能となる。従って、キー更新処理によって新しいバージョンのＫＲＢを不正な機器をリバークして発行することにより、その後は、正当な機器のみが取得可能な新しいバージョンのＫＲＢから取得されるキーに基づく暗号化コンテンツを記録媒体に格納することが可能となるので、記録媒体自体の世代に関わらず、新規格納される暗号化コンテンツに関しては、リバークされた機器における利用排除が可能となる。

【０１８５】また、本発明の情報記録再生装置によれば、記録再生装置にはどんどん新しいＫＲＢが格納されることになり、またデータが記録される際には、その時点で記録再生装置と記録媒体が格納する最新のＫＲＢにより算出されるメディアキーを用いてデータが暗号化されて記録されるから、たとえ記録媒体が製造されたのがとても古く、あらかじめ記録媒体に格納されているＫＲＢが古いものであったとしても、データが記録される際には新しいＫＲＢが使われ、暗号化コンテンツはより新しいバージョンの暗号処理キーで暗号化されることになる。このため、本発明によれば、映画や音楽などの著作権があるデータの不正な複製、例えば著作権者の意に反する複製が蔓延することを防ぐことができる。

【図面の簡単な説明】

【図１】本発明の情報記録再生装置の構成例を示すブロック図である。

【図２】本発明の情報記録再生装置のデータ記録処理フローを示す図である。

【図３】本発明の情報記録再生装置のデータ再生処理フローを示す図である。

【図４】本発明の情報記録再生装置に対するメディアキー等の鍵の暗号化処理について説明するツリー構成図である。

【図５】本発明の情報記録再生装置に対するメディアキー等の鍵の配布に使用されるキー更新ブロック（ＫＲＢ）の例を示す図である。

【図６】情報記録再生装置におけるメディアキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理例を示す図である。

【図７】本発明の情報記録再生装置におけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図である。

【図８】本発明の情報記録再生装置において適用可能なディスク固有キーの生成例を説明する図である。

【図９】本発明の情報記録再生装置において、適用可能なタイトル固有キーの生成処理例を示す図である。

【図１０】本発明の情報記録再生装置において適用可能なブロック・キーの生成方法を説明する図である。

【図１１】本発明の情報記録再生装置におけるメディアキーを使用したデータ再生処理時の復号処理を説明するブロック図である。

【図１２】本発明の情報記録再生装置において使用されるキー更新ブロック（ＫＲＢ）のフォーマット例を示す図である。

【図１３】本発明の情報記録再生装置において使用されるキー更新ブロック（ＫＲＢ）のタグの構成を説明する図である。

【図１４】本発明の情報記録再生装置においてキー更新ブロック（ＫＲＢ）を複数格納した記録媒体、および記

録再生装置におけるキー更新ブロック（ＫＲＢ）の更新処理を説明する図である。

【図１５】本発明の情報記録再生装置におけるキー更新ブロック（ＫＲＢ）の更新処理を説明するフロー図である。

【図１６】本発明の情報記録再生装置においてキー更新ブロック（ＫＲＢ）を複数格納した記録媒体、および最新のキー更新ブロック（ＫＲＢ）を用いて取得されるキーによる暗号化を行なったコンテンツの格納処理を説明する図である。

【図１７】本発明の情報記録再生装置におけるキー更新ブロック（ＫＲＢ）を用いて取得されるキーによる暗号化、コンテンツの格納処理を説明するフロー図である。

【図１８】本発明の情報記録再生装置におけるキー更新ブロック（ＫＲＢ）を用いて取得されるキーによる復号、およびコンテンツの再生処理手順を説明するフロー図である。

【図１９】本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

【図２０】本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

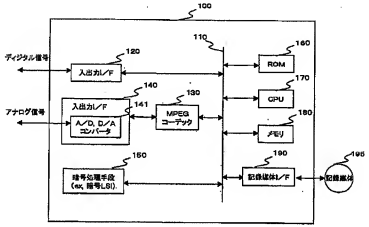
【図２１】本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

【符号の説明】

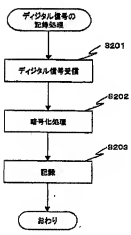
１００　記録再生装置
１１０　バス
１２０　入出力Ｉ／Ｆ
１３０　ＭＰＥＧコーデック
１４０　入出力Ｉ／Ｆ
１４１　Ａ／Ｄ，Ｄ／Ａコンバータ
１５０　暗号処理手段
１６０　ＲＯＭ
１７０　ＣＰＵ

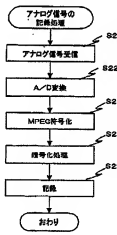
１８０　メモリ
１９０　ドライブ
１９５　記録媒体
７００　記録再生装置
７０１　メディアキー
７０２　記録媒体
１２０１　バージョン
１２０２　デプス
１２０３　データポインタ
１２０４　タグポインタ
１２０５　署名ポインタ
１２０６　データ部
１２０７　タグ部
１２０８　署名
１４１０　記録再生装置
１４１１，１４１２　キー更新ブロック（ＫＲＢ）
１４２０　記録媒体
１４２１，１４２２　キー更新ブロック（ＫＲＢ）
１４３１，１４３２　コンテンツ
１６４１０　記録再生装置
１６１１　キー更新ブロック（ＫＲＢ）
１６２０　記録媒体
１６２１，１６２２　キー更新ブロック（ＫＲＢ）
１６３１，１６３２　コンテンツ
２１０１　バス
２１０２　ＣＰＵ
２１０３　ＲＯＭ
２１０４　ＲＡＭ
２１０５　ハードディスク
２１０６　出力部
２１０７　入力部
２１０８　通信部
２１０９　ドライブ
２１１０　リムーバブル記録媒体
２１１１　入出力インタフェース

【図１】



【図２】





【図５】

(A) キー更新ブロック(KRB:Key Renewal Block) 例1

デバイス0, i, 2には時点でのルートキーK(t)Rを送付

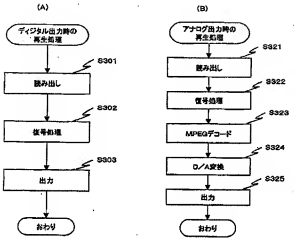
世代(Generation):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)000)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) キー更新ブロック(KRB:Key Renewal Block) 例2

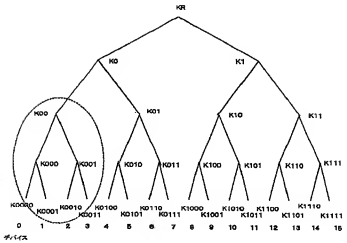
デバイス0, 1, 2には時点でのルートキーK(t)Rを送付

世代(Generation):t	
インデックス	暗号化キー
000	Enc(K000, K(t)000)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

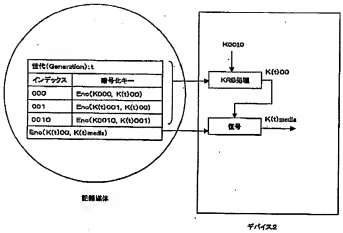
【図３】


(A)
ディジタル出力時の再生処理
S301
読み出し
S302
復号処理
S303
出力
おわり
(B)
アナログ出力時の再生処理
S321
読み出し
S322
復号処理
S323
MPEGデコード
S324
D／A変換
S325
出力
おわり

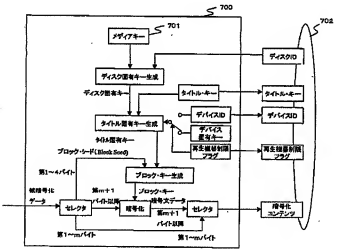
【図４】


KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
ディバイス

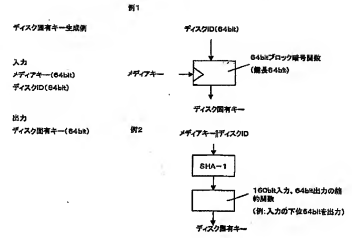
【図６】


世代(Generation):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)
K0010
KRB処理
K(t)00
復号
K(t)media
記録媒体
デバイスB

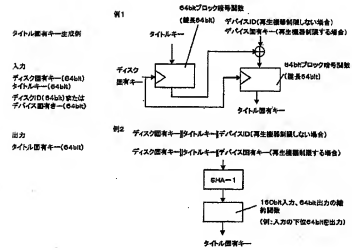
【図７】


700
701
702
メディアキー
ディスクID
ディスク固有キー生成
ディスク固有キー
タイトル・キー
タイトル・キー
デバイスID
デバイスID
タイトル固有キー生成
デバイス固有キー
64bit固有キー
再生経路制御プログラム
再生経路制御プログラム
ブロック・シード(Block Seed)
第1～4バイト
ブロック・キー生成
ブロック・キー
暗号化データ
セレクタ
暗号化
セレクタ
暗号化コンテンツ
第1～mバイト
第1～mバイト

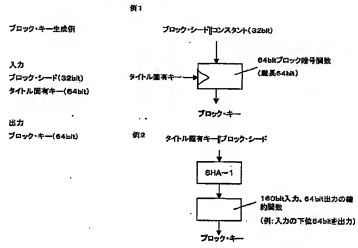
【図８】


例1
ディスク固有キー生成例
ディスクID(64bit)
入力
メディアキー(64bit)
ディスクID(64bit)
メディアキー
64bitブロック暗号関数
(鍵長64bit)
ディスク固有キー
出力
ディスク固有キー(64bit)
例2
メディアキー‖ディスクID
SHA－1
160bit入力、64bit出力の縮約関数
(例:入力の下位64bitを出力)
ディスク固有キー

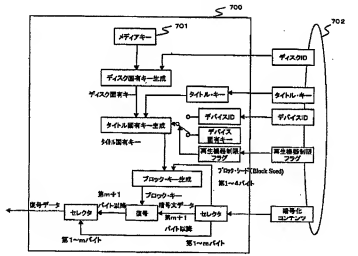
【図９】


例1
64bitブロック暗号関数
(鍵長64bit)
タイトル固有キー生成例
ディバイスID(再生機器制限しない場合)
ディバイス固有キー(再生機器制限する場合)
タイトルキー
入力
ディスク固有キー(64bit)
タイトルキー(64bit)
ディスクID(64bit)またはディバイス固有キー(64bit)
ディスク固有キー
64bitブロック暗号関数
(鍵長64bit)
タイトル固有キー
出力
タイトル固有キー(64bit)
例2
ディスク固有キー‖タイトルキー‖ディバイスID(再生機器制限しない場合)
ディスク固有キー‖タイトルキー‖ディバイス固有キー(再生機器制限する場合)
SHA－1
160bit入力、64bit出力の縮約関数
(例:入力の下位64bitを出力)
タイトル固有キー

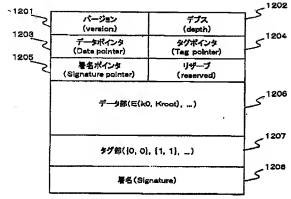
【図１０】


例1
ブロック・キー生成例
ブロック・シード||コンスタント(32bit)
入力
ブロック・シード(32bit)
タイトル固有キー(64bit)
出力
ブロック・キー(64bit)
タイトル固有キー
64bitブロック暗号関数
(鍵長64bit)
ブロック・キー
例2
タイトル固有キー||ブロック・シード
SHA－1
160bit入力、64bit出力の縮約関数
(例:入力の下位64bitを出力)
ブロック・キー

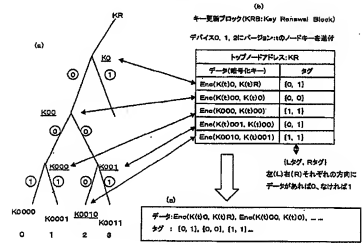
【図１１】


700
701
702
メディアキー
ディスクID
ディスク固有キー生成
ディスク固有キー
タイトル・キー
タイトル・キー
デバイスID
デバイスID
タイトル固有キー生成
タイトル固有キー
デバイス鍵情報
再生機器制御フラグ
再生機器制御フラグ
ブロック・キー生成
ブロック・シード(Block Seed)
第1～mバイト
第m+1バイト
ブロック・キー
暗号データ
バイト加算
暗号データ
セレクタ
復号
第m+1バイト
セレクタ
暗号化コンテンツ
バイト加算
第1～mバイト
第1～mバイト

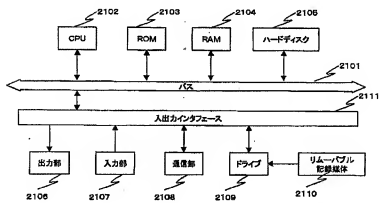
【図１２】


1201
バージョン (version)
デプス (depth)
1202
1203
データポインタ (Data pointer)
タグポインタ (Tag pointer)
1204
1205
署名ポインタ (Signature pointer)
リザーブ (reserved)
データ部(={k0, Kroot}, ...)
1206
タグ部({0, 0}, {1, 1}, ...)
1207
署名(Signature)
1208

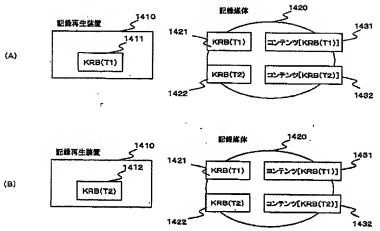
【図１３】


(b)
キー更新ブロック(KRB:Key Renewal Block)
デバイスの、1、2にバージョンnのノードキーを送付
KR
(a)
K0
K00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
トップノードアドレス:KR
データ(暗号化キー)
タグ
Enc(K(k)0, K(t)R)
{0, 1}
Enc(K(k)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(k)001, K(t)100)
{0, 1}
Enc(K0010, K(k)0001)
{1, 1}
(L)タグ、(R)タグ
左(L)右(R)それぞれの方向にデータがあれば0、なければ1
(a)
データ:Enc(K(k)0, K(t)R), Enc(K(t)00, K(t)0), ...
タグ : {0, 1}, {0, 0}, {1, 1}...

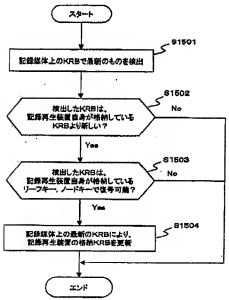
【図２１】


2102
2103
2104
2105
CPU
ROM
RAM
ハードディスク
2101
バス
2111
入出力インタフェース
出力部
入力部
通信部
ドライブ
リムーバブル 記録媒体
2106
2107
2108
2109
2110

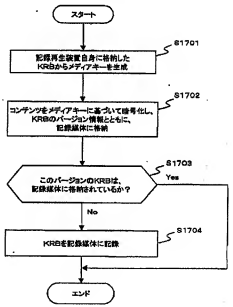
【図１４】


(A)
記録再生装置
1410
1411
KRB(T1)
記録媒体
1420
1421
KRB(T1)
コンテンツ[KRB(T1)]
1431
KRB(T2)
コンテンツ[KRB(T2)]
1422
1432
(B)
記録再生装置
1410
1412
KRB(T2)
記録媒体
1420
1421
KRB(T1)
コンテンツ[KRB(T1)]
1431
KRB(T2)
コンテンツ[KRB(T2)]
1422
1432

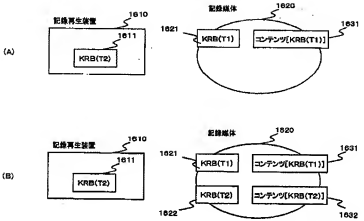
【図１５】


スタート
S1501
記録媒体上のKRBで最新のものを検出
S1502
検出したKRBは、記録再生装置自身が格納しているKRBより新しい？
No
Yes
S1503
検出したKRBは、記録再生装置自身が格納しているリーフキー、ノードキーで復号可能？
No
Yes
S1504
記録媒体上の最新のKRBにより、記録再生装置の格納KRBを更新
エンド

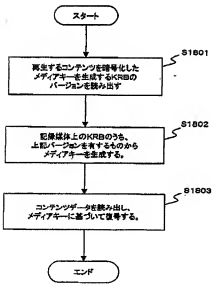
【図１７】


スタート
S1701
記録再生装置自身に格納したKRBからメディアキーを生成
S1702
コンテンツをメディアキーに基づいて暗号化し、KRBのバージョン情報とともに、記録媒体に格納
S1703
このバージョンのKRBは、記録媒体に格納されているか？
Yes
No
S1704
KRBを記録媒体に記録
エンド

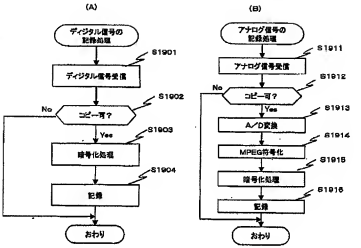
【図１６】


(A)
記録再生装置
1610
1611
KRB(T2)
記録媒体
1620
1621
KRB(T1)
コンテンツ[KRB(T1)]
1631
(B)
記録再生装置
1610
1611
KRB(T2)
記録媒体
1620
1621
KRB(T1)
コンテンツ[KRB(T1)]
1631
KRB(T2)
コンテンツ[KRB(T2)]
1622
1632

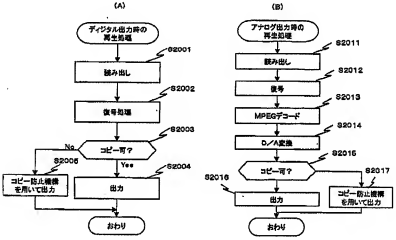
【図１８】


スタート
S1801
再生するコンテンツを暗号化した
メディアキーを生成するKRBの
バージョンを読み出す
S1802
記録媒体上のKRBのうち、
上記バージョンを有するものから
メディアキーを生成する。
S1803
コンテンツデータを読み出し、
メディアキーに基づいて復号する。
エンド

【図１９】



【図２０】



フロントページの続き

(72)発明者 石黒 隆二
東京都品川区北品川６丁目７番35号 ソニー株式会社内
(72)発明者 光澤 敦
東京都品川区北品川６丁目７番35号 ソニー株式会社内
(72)発明者 大石 丈於
東京都品川区北品川６丁目７番35号 ソニー株式会社内

Ｆターム(参考) 5B017 AA07 BA07 CA16
5D044 AB05 AB07 BC04 BC08 CC06 CC09 DE47 DE50 DE59 EF05 FG18 GK12 HH13 HH15 HL08
5J104 AA01 AA16 EA01 EA07 EA17 EA24 NA02 PA14